U.S. General Services Administration Information Technology Category (ITC)

Executive Order 14028: Improving the Nation's Cybersecurity.

Request for Information

December 21, 2021

A. Synopsis

THIS IS A REQUEST FOR INFORMATION (RFI). This is NOT a solicitation for proposals, proposal abstracts, or quotations. The purpose of this RFI is to obtain knowledge and information for project planning purposes, exploring alternative solutions and determining industry best practices for implementing Executive Order 14028: Improving the Nation's Cybersecurity.

B. Background

On May 12, 2021, President Biden signed an Executive Order to improve the nation's cybersecurity and protect federal government networks. The Scope of the EO spans across IT and OT systems no matter the type of operating environment (on prem, off-prem, hybrid). Specifically, the Executive Order:

- Requires service providers to share cyber incident and threat information that could impact Government networks.

- Moves the Federal government to secure cloud services, zero-trust architecture, and mandates deployment of multifactor authentication and encryption within a specific time period.

- Establishes baseline security standards for development of software sold to the government, including requiring developers to maintain greater visibility into their software and making security data publicly available.

- Establishes a Cybersecurity Safety Review Board, co-chaired by government and private sector leads, that may convene following a significant cyber incident to analyze what happened and make recommendations for improving cybersecurity.

- Creates a standardized playbook and set of definitions for cyber incident response by Federal departments and agencies.

- Improves the ability to detect malicious cyber activity on Federal networks by enabling a government-wide endpoint detection and response system and improved information sharing within the Federal government.

- Creates cybersecurity event log requirements for Federal departments and agencies.

- Requires amendments to the FAR to align with requirements in the EO.

Resources:

- Executive Order 14028, *Improving the Nation's Cybersecurity*
- NIST Definition of Critical Software
- OMB M-21-30, *Protecting Critical Software Through Enhanced Security Measures*
- OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*
- *M-22-01 Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*
- Moving the U.S. Government Towards Zero Trust Cybersecurity Principles
- NIST frameworks and controls for risk management, security and privacy, zero trust, and supply chain
- Information on the development of Federal regulations

C. Questions for Industry -

GSA is assessing the impact of the subject EO on the small business community through obtaining feedback from industry regarding the areas listed above.

D. Responses Requested

All responses must be provided no later than **January 31, 2022** and submitted through RFI Executive Order 14028 Form only. A copy of your response will be sent to the email address provided.

E. Use of Results and Confidentiality

The release of this RFI does not guarantee that the government will, in the end, complete an acquisition or create a new SIN. This RFI is for information and planning purposes only and does not constitute a solicitation for bids, proposals or quote and is not to be construed as a commitment by the government to issue a request for proposal/quote or award of a contract as a result of this request. **This announcement is not a Request for Proposal (RFP) or a Request for Quote (RFQ).** The government will not reimburse respondents for any cost associated with information submitted in response to this request.

Any document submitted in response to this RFI that contains confidential information must be marked on the outside as containing confidential information. Each page upon which confidential information appears must be marked as containing confidential information. The confidential information must be clearly identifiable to the reader wherever it appears. All other information will not be treated as confidential.

All information marked confidential in RFI responses is only for the government's planning use. Confidential information may be reviewed by contractors providing advisory services within scope of contract, subject to a non-disclosure agreement (NDA) including but not limited to commercial or financial data obtained from or contained in contractor/vendor submitted documents and proposals. Otherwise, no information marked confidential included in this document or in discussions connected to it may be disclosed to any other party outside of the government.

For more information, please contact: gsasrmteam@gsa.gov

(end)